



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/660,370	09/12/2000	Thomas P. Hardjono	2204/A55	6652

2101 7590 07/28/2004  
BROMBERG & SUNSTEIN LLP  
125 SUMMER STREET  
BOSTON, MA 02110-1618

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

4

# Office Action Summary

Application No.

09/660,370

Applicant(s)

HARDJONO, THOMAS P.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 12 September 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-69 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-69 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

Art Unit: 2134

### **DETAILED ACTION**

1. This office action is in response to applicant's application serial no. 09/660,370 filed on 9/12/2000.

#### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 66-69 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim language merely recites a description of a communication message. A broadest reasonable interpretation of the claim would include a non-computer implementation of the recited limitation.

#### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Mitra (U.S. Patent No. 5,748,736).

In respect to claim 13, Mitra discloses method comprising:

Art Unit: 2134

authenticating a host device; generating an authentication key for the host device; and sending the authentication key to the host device and to a rendezvous point device using a secure key distribution mechanism mechanism (see Mittra, col. 4, lines 7-25 and col. 7, line 26-col. 8, line 35 and col. 12, lines 50-59).

In respect to claims 14 and 15, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claim 13. Therefore, claims 14 and 15 are rejected based on the similar rationale.

In respect to claims 16 and 17, Mittra discloses the computer readable medium of claim 15, wherein the computer readable medium is a computer storage medium and a computer communication medium (see Mittra, col. 6, lines 1-19).

4. Claims 48-64 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta (U.S. Patent No. 6,718,387).

In respect to claim 48, Gupta discloses a method comprising:

Receiving an encoded join request for a host device; authenticating the encoded join request to determine whether or not the encoded joint message is authentic; and establishing appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the join request is determined to be authentic (see Gupta, col. 6, line 9-44).

In respect to claim 49, Gupta discloses the method of claim 48, wherein authenticating the encoded join request comprises:

maintaining a number of authentication keys; determining the host device for the encoded join request; and searching for an authentication key associated with the host device (see Gupta, col. 6, lines 9-44).

In respect to claim 50, Gupta discloses the method of claim 49, wherein authenticating the encoded join request further comprises:

    failing to find an authentication key associated with the host device; and  
    determining that the encoded join request is not authentic (see Gupta, col. 6, lines 9-44).

In respect to claim 51, Gupta discloses the method of claim 49, wherein authenticating the encoded join request further comprises:

    finding an authentication key associated with the host device; and  
    authenticating the encoded join request using the authentication key associated with the host device (see Gupta, col. 6, lines 9-44).

In respect to claim 52, Gupta discloses the method of claim 48, further comprising:

    sending an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic (see Gupta, col. 6, lines 9-44).

In respect to claims 53-62, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claims 48-52.

Therefore, claims 53-62 are rejected based on the similar rationale.

Art Unit: 2134

In respect to claims 63-64, Gupta discloses the computer readable medium of claim 58, wherein the computer readable medium is a computer storage medium and a communication medium (see Gupta, col. 2, lines 21-42).

5. Claim 66 is rejected under 35 U.S.C. 102(b) as being anticipated by Ballardie (Network Working Group, University College of London, May 1996).

In respect to claim 66, Ballardie discloses a communication message embodied in a data signal, the communication message comprising a group key for a multicast group and an authentication key for a host device (see page 11).

6. Claim 67 is rejected under 35 U.S.C. 102(b) as being anticipated by Fan (U.S. Patent No. 6,664,922).

In respect to claim 67, Fan discloses a communication message embodied in a data signal, the communication message comprising a join request including an authentication key for a host device (see Fan, col. 9, lines 20-39).

### ***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2134

Claims 1-4 and 7-12 and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,738) in view of Gupta et al. (U.S. Patent No. 6,718,387) and further in view of Ballardie (Network Working Group, University College of London, May 1996).

In respect to claim 1, Mittra discloses a communication system comprising:

a rendezvous point device that forwards multicast communication messages to members of a shared tree; a designated device in communication with the rendezvous point device via a number of intermediate devices (see col. 12, lines 50-59); and

a host device in communication with the designated device, wherein the host device sends a join request to the designated device in order to join the shared tree for receiving the multicast communication messages forwarded by the rendezvous point device; and the host device is prevented from receiving the multicast communication messages forwarded by the rendezvous point device, if the rendezvous point device determines that the join message is not authentic (see Abstract, col. 4, lines 6-25 and col. 12, lines 50-59).

Mittra does not explicitly disclose but Gupta discloses the host device sends an encoded join request generated using an authentication key associated with the host device using a predetermined multicast group management protocol (see Gupta, col. 6, lines 9-44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Mittra's secure group communication via multicast with the teaching of Gupta's encoded join request in order

Art Unit: 2134

to prevent unauthorized user from gaining access to a multicast by duplicating other's join request (Gupta, col. 6, lines 17-21).

Mittra does not explicitly disclose but Ballardie discloses the designated device receives the join request and forwards to the primary core of a core basic tree (CBT) via the number of intermediate devices (see Ballardie, page 8 to page 12, section 6.2). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Mittra's secure group communications via multicast with Ballardie's teaching of forwarding the join request from the secondary device to the primary device via a number of intermediate devices so that the host can send the join request to its local multicast router (Ballardie, page 9, 4<sup>th</sup> paragraph).

In respect to claim 2, Mittra, Gupta and Ballardie disclose the communication system of claim 1, further comprising a key server for authenticating the host device and generating the authentication key for the host device (see Mittra, col. 4, lines 7-25 and col. 7, line 26-col. 8, line 35).

In respect to claim 3, Mittra, Gupta and Ballardie disclose the communication system of claim 2, wherein the key server provides the authentication key to both the host device and other router element using a secure key distribution mechanism (see Mittra, col. 4, lines 7-25 and col. 7, line 26-col. 8, line 35 and col. 12, lines 50-59).

In respect to claim 4, Mittra, Gupta and Ballardie disclose the communication system of claim 1, wherein the host device sends the authentication key to the designated device (see Gupta, col. 6, lines 9-44).



In respect to claim 7, Mitra, Gupta and Ballardie disclose the communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device (see Ballardie, page 9 to page 12 ).

In respect to claim 8, Mitra, Gupta and Ballardie disclose the communication system of claim 7, wherein the designated device establishes appropriate multicast routes for forwarding multicast communication messages to the host (see Ballardie, page 9 to page 12).

In respect to claim 9, Mitra, Gupta and Ballardie disclose the communication system of claim 1, wherein each intermediate device receives the encoded join request and forwards the encoded join request toward other routing element (see Gupta, col. 6, lines 9-44).

In respect to claim 10, Mitra, Gupta and Ballardie disclose the communication system of claim 9, wherein each intermediate device that is not already joined to the shared tree joins the shared tree on behalf of the host device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device upon receiving the join request (see Ballardie, page 9 to page 12).

In respect to claim 11, Mitra, Gupta and Ballardie disclose the communication system of claim 9, wherein each intermediate device that is already joined to the shared tree waits for an explicit acknowledgment message from the primary router and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the primary router (see Ballardie, page 9 to page 12).

Art Unit: 2134

In respect to claim 12, Mittra, Gupta and Ballardie disclose the communication system of claim 1, wherein the primary router sends an explicit acknowledgment message toward the host device upon determining that the join request is authentic (see Ballardie, page 9 to page 12).

In respect to claim 65, the claim limitation is substantially similar to claim 1. Therefore, claim 65 is rejected based on the similar rationale.

8. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,738), Gupta et al. (U.S. Patent No. 6,718,387) and Ballardie (Network Working Group, University College of London, May 1996) as applied to claim 4 above, and further in view of Fan (U.S. Patent No. 6,664,922).

In respect to claims 5 and 6, Mittra, Gupta and Ballardie disclose the communication system of claim 4. Gupta discloses wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) (Gupta, col. 6, lines 9-44) but do not explicitly disclose wherein the host device sends the authentication key to the designated device in the join request. However, Fan discloses a sending device sends the authentication key to the designated device a request provided with an authentication key over a data network (see Fan, col. 9, lines 20-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Mittra, Gupta and Ballardie's teaching of a secure joining in a multicast communication with Fan's teaching of including authentication key in a request to the destination device so that the

Art Unit: 2134

identity of the requesting device can be verified and the key can be used to provide requesting device access to data content (Fan, col. 9, lines 22-25).

9. Claims 18-19 and 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6718387) in view of Fan (U.S. Patent No. 6,664,922).

In respect to claims 18 and 19, Gupta discloses a method comprising:

obtaining an authentication key; and sending a join request to a designated device using a predetermined multicast group management protocol wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) (see Gupta, col. 6, lines 9-44) but does not disclose the join request including the authentication key. However, Fan discloses request sent to the destination device is provided with an authentication key (see Fan, col. 9, lines 20-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Gupta's teaching of a secure joining in a multicast communication with Fan's teaching of including authentication key in a request to the destination device so that the identity of the requesting device can be verified and the key can be used to provide requesting device access to data content (Fan, col. 9, lines 22-25).

In respect to claims 20-23, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claims 18-19.

Therefore, claims 20-23 are rejected based on the similar rationale.

Art Unit: 2134

In respect to claims 24 and 25, Gupta and Fan disclose the computer readable medium of claim 22, wherein the computer readable medium is a computer storage medium and a computer communication medium (see Gupta, col. 4, lines 60-67).

10. Claims 26, 29, 32, 37, 40, 43 and 46-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,738) in view of Gupta et al. (U.S. Patent No. 6718387).

In respect to claim 26, Mittra discloses a method comprising:

receiving a join request from a host device and sending the encoded join request toward a rendezvous point device (see Mittra, col. 4, lines 7-25 and col. 7, line 26-col. 8, line 35 and col. 12, lines 50-59).

Mittra does not disclose but Gupta discloses generating an encoded join request using an authentication key associated with the host device (see Gupta, col. 6, lines 9-44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Mittra's secure group communication via multicast with the teaching of Gupta's encoded join request in order to prevent unauthorized user from gaining access to a multicast by duplicating other's join request (Gupta, col. 6, lines 17-21).

In respect to claims 29 and 32, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claim 26. Therefore, claims 29 and 32 are rejected based on the similar rationale.

Art Unit: 2134

In respect to claims 37, 40 and 43, the claim limitations are substantially similar to claim 26. Therefore, claims 37, 40 and 43 are rejected based on the similar rationale.

In respect to claims 46-47, Mittra and Gupta disclose the computer readable medium of claim 43, wherein the computer readable medium is a computer storage medium and a computer communication medium (see Mittra, col. 6, lines 4-19).

11. Claims 27, 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,738) in view of Gupta et al. (U.S. Patent No. 6,718,387) as applied to claim 26 above and further in view of Fan (U.S. Patent No. 6,664,922).

In respect to claim 27, Mittra and Gupta disclose the method of claim 26. Mittra and Gupta does not disclose a request sends to a destination device includes an authentication key. However, Fan discloses request sent to the destination device is provided with an authentication key (see Fan, col. 9, lines 20-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Gupta's teaching of a secure joining in a multicast communication with Fan's teaching of including authentication key in a request to the destination device so that the identity of the requesting device can be verified and the key can be used to provide requesting device access to data content (Fan, col. 9, lines 22-25).

Art Unit: 2134

In respect to claims 30 and 33, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claim 27. Therefore, claims 30 and 33 are rejected based on the similar rationale.

12. Claims 28, 31, 34, 38-39, 41-42 and 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,738) in view of Gupta et al. (U.S. Patent No. 6718387) as applied to claim 26 above and further in view of Ballardie (Network Working Group, University College of London, May 1996).

In respect to claim 28, Mittra and Gupta disclose the method of claim 26. Mittra and Gupta does not explicitly disclose but Ballardie discloses joining a shared tree on behalf of the host device and establishing appropriate multicast routes for forwarding multicast communication messages to the host device (see Ballardie, page 9 to page 12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Mittra and Gupta's secure joining of multicast communication with the teaching of Ballardie to joining a shared tree on behalf of the host device in establishing a multicast communication for a secure joining process (see Ballardie, page 21 last paragraph).

In respect to claims 31 and 34, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claim 28. Therefore, claims 31 and 34 are rejected based on the similar rationale.

In respect to claims 35 and 36, Mittra and Gupta disclose the computer readable medium claim 32, wherein the computer readable medium is a computer storage medium and a computer communication medium (see Mittra, col. 6, lines 3-19).

In respect to claims 38, 41 and 44, the claim limitations are substantially similar to claim 28. Therefore, claims 38, 41 and 44 are rejected based on the similar rationale.

In respect to claim 39, Mittra and Gupta disclose the method of claim 37. Mittra and Gupta do not disclose waiting for an explicit acknowledgment message from the primary core; and establishing appropriate multicast router for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device (see Ballardie, page 9 to page 12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Mittra and Gupta's secure joining of multicast communication with the teaching of Ballardie's authenticating host with acknowledgement message from primary core for a secure joining of a shared tree (Ballardie, page 2, 3<sup>rd</sup> paragraph).

In respect to claims 42 and 45, the claim limitations are apparatus and computer readable medium claims that are substantially similar to method claim 39. Therefore, claims 42 and 45 are rejected based on the similar rationale.

13. Claim 68 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6718387) in view of Arbaugh et al. (U.S. Patent No. 6,185,678).

In respect to claim 68, Gupta discloses a communication message embodied in a data signal, the communication message comprising an encoded join request (see Gupta, col. 6, lines 31-44). Gupta does not explicitly disclose but Arbaugh discloses a message including a tag field and a nonce field (see Arbaugh, col. 14, lines 16-32 and col. 16, lines 15-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Gupta's secure joining in a multicast with Arbaugh's teaching of including tag field and nonce field in the message in order to detect integrity failure of the message transmitted over the network (see Arbaugh, col. 3, lines 25-39).

14. Claim 69 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ballardie (Network Working Group, University College of London, May 1996) as applied to claim 4 above, and further in view of Arbaugh et al. (U.S. Patent No. 6,185,678).

In respect to claim 69, Gupta discloses a communication message embodied in a data signal, the communication message comprising an explicit acknowledgment (see Ballardie, page 11). Gupta does not explicitly disclose but Arbaugh discloses a message including a tag field and a nonce field ((see Arbaugh, col. 14, lines 16-32 and col. 16, lines 15-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Gupta's secure joining in a multicast with Arbaugh's teaching of including tag field and nonce field in the message in order to detect integrity failure of the message transmitted over the network (see Arbaugh, col. 3, lines 25-39).



### ***Conclusion***

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Li discloses a hierarchical multicast traffic security system in an internetwork.

-Aziz discloses a method and apparatus for sending secure datagram multicast.

-Srivastava disclose method and apparatus for distributing and updating group controllers over a wide area network using a tree structure.

-Peyravian et al. Disclose a decentralized system methods and computer program products for sending secure messages among a group of nodes.

-McCanne et al. Disclose proximity based redirection system for robust and scalable service node location in an internetwork.

-Mukherjee et al. Disclose a flexible state sharing and consistency mechanism for interactive applications.

-Kadansky et al. Disclose a method and apparatus for multicast indication of group key change.

-Haller discloses authentication requirements of computer system and network protocol.

-Harney discloses Group Key Management Protocol specification.

-Gong et al. Discloses elements of trusted multicasting.

-Mittra discloses a framework for scalable secure multicasting.

-Ishikawa et al. Disclose an architecture for user authentication of IP multicast and its implementation.

Art Unit: 2134


16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran  
Art Unit: 2134

TT

  
July 15, 2004

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100